UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/578,633	05/25/2000	Steven Branigan	1-1-7	5753

22046 7590 03/08/2005

LUCENT TECHNOLOGIES INC.
DOCKET ADMINISTRATOR
101 CRAWFORDS CORNER ROAD - ROOM 3J-219
HOLMDEL, NJ 07733

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/578,633	BRANIGAN ET AL.	
	Examiner	Art Unit	
	Syed Zia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *26 November 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,6-12,14-24,26 and 27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,6-12,14-24,26 and 27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to amendment filed on November 26, 2004. Original application contained Claims 1-27. Applicant previously amended Claims 1-2, 6-11, 14,15, 6, 18-24, and 26-27. Applicant previously cancelled 4-5, 13, and 25. Applicant argument filed on November 26, 2004 have been entered and made of record. Therefore, presently pending claims are 1-3, 6-12, 14-24, and 26-27.

Response to Arguments

Applicant's arguments filed November 26, 2004 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1, 10, 16, 21, and 24 applicants argued that in the cited prior art (CPA) [Shostack (U.S. Patent No. 6,298,445) "*second module (and, for that matter fourth module) as highlighted in the Office Action is not performing (and does not anticipate, teach or suggest) Applicants' claimed invention. In particular, the fact that Shostack's fourth module essentially implements --on a remote basis--the functionality of the second module does not teach or suggest Applicants' claimed invention. Applicants' claimed invention is directed at discovering—as function of the sending/receiving of the claimed probe packet --connectivity of, or between, a host machine (or host machines) not whether such host (or hosts) is susceptible to IP spoofing* ".

And also argued that "*Applicants find no teaching or suggestion in Shostack's sixth module with respect to the aspect of Applicants' claimed invention directed to utilizing a probe packet to determine a connectivity measure between two communication networks (where the packet includes a source address which is associated with a second communications network*".

This is not found persuasive. The system of cited prior art teaches and describes a computer security system modules for accessing security vulnerabilities on networks such as internet, intranet, extranet, etc. where modules (74,76,78) are used for accessing a data base and the security vulnerability of a computer network, and modules (88,90) are used for accessing security vulnerability of a remote computer connected to the network and for receiving and updating to data base respectively.

Cited prior art teaches a fourth module of this system which allows a remote computer to first connect to a network service and like the second network module, interrogates the service. Examiner references column 12, lines 41-57 as the teaching of what module two does. Specifically module two carries out the network scan and generates a map of the network and scans the ports for known security vulnerabilities. Therefore module four does this from a remote location. The remote location would then have a source address associated with a second communications network. An address that is different from the first communications network. Cited prior art also teaches a sixth module which is a communication module that allows an integrated security system to communicate with a similar system over a computer network. In line 27, the module invokes remote systems. In line 34, Shostack teaches that this sixth checks the integrity of the service connection. This teaching is another example of communication between networks to perform the security functions

of cited prior art invention.

The examiner has pointed to two separate teachings where cited prior art teaches or suggests utilizing a probe packet to determine a connectivity measure between the two communication networks where the packet includes a source address which is associated with a second communication network.

Therefore, the examiner asserts that user obtains instant access to the latest security vulnerabilities and employs immediate remedial action before a security breach occurs, and automatic enhancements are made for the database of security vulnerabilities, thus providing a security solution to potential weak computer or computer network. Thus, the system of prior art provides robustness of security measures and ensuring that network security features are universally configured throughout a commemorations network.

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. The examiner is not trying to interpret the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that the system of cited prior arts does teach or suggest the subject matter broadly recited in independent Claim 1, 10, 16,21,and 24 and in subsequent dependent Claims. Accordingly, rejections for claims 1-3, 6-12, 14-24, and 26-27 are respectfully maintained.

Claim Objections

Claim 6 is objected to because of the following informalities: Claim 6 is dependent on a cancelled Claim. Appropriate correction is required. Examiner assumed that this claim is dependent on Claim 3.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

1. Claim 1,10, 16, 21, and 24 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The subject matters "security characteristic" and "an indication of connectivity" is not enabled in the specification, and it is not clear what is being measured regarding security characteristic of the probed network when measuring characteristic is only an indication of connectivity. Is measure of indication of connectivity pertains to available bandwidth, traffic load or the integrity of the network? .

2. Claim 7, 20, and 23 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The limitation "different security levels" is not defined and described in the specification. Does "different security levels" means access authentication for users, or security policy implemented on the network in general and on firewall in particular?

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1-3, 6-12, 14-24, and 26-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Shostack et al (USP 6,298,445).

As per claims 1 and 24, Shostack et al teach a communications network security method comprising:

identifying a plurality of routes that define the communications network

(column 12, lines 41-57),

identifying a plurality of hosts as a function of the plurality of routes (column 12, lines 41-57),

performing a census of the communications network as a function of the plurality of hosts to determine a topology of the communications network (column 12, lines 41-57);

probing at least one host of the plurality hosts by transmitting a packet to the host, the host being selected from the census results and the packet having at least a source address determined as a function of the topology (column 12, lines 41-57), and

determining a security characteristic of the probed host as a function of a response by the probed host in receiving the packet, the security characteristic being a measure of connectivity between the first communications network and the second communications network (column 12, lines 41-57 and column 13, lines 1-5).

As per claims 2 and 14, Shostack et al teach the source address is an IP address associated with a host external to the communications network (column 1, lines 64-65 and column 3, lines 1-4).

As per claims 3 and 26, Shostack et al teach the response of the probed host to the receipt of the packet includes transmitting a second packet, the second packet being derived using at least a portion of information from the received packet (column 5, lines 20-35).

As per claim 6, Shostack et al teach the determining the security characteristic operation further comprises:

monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a security alert message identifying the probed host as a security risk (column 7, lines 5-19).

As per claim 7, Shostack et al teach the first and second communications network have different security levels (column 13, lines 1-5).

As per claim 8, Shostack et al teach the transmitted packet is a TCP packet (column 5, lines 24-45).

As per claim 9, Shostack et al teach the second packet is a UDP packet or an ICMP packet (column 5, lines 24-45).

As per claim 10, Shostack et al teach a method for analyzing network security of a communications network, the method comprising:

identifying a plurality of routes that define the communications network (column 12, lines 41 -57);

Identifying a plurality of hosts internal to the communications network as a function of the plurality of routes (column 12, lines 41-57),

performing a census of the communications network as a function of the plurality of hosts to determine a topology of the communications network (column 1 2, lines 41-57);

transmitting a packet from a host external to the communications network to a particular one host of the plurality of hosts internal to the communications network, the internal host being selected from the census, and the packet being generated as a function of an IP address associated with the host external to the communications network and an IP address associated with the particular one host of the plurality of hosts internal to the communications network (column 13, lines 1-6); and

determining a security characteristic of the particular one internal host as a function of a response by the internal host to the receipt of the packet, the security characteristic being a measure of connectivity between the first communications network and the second communications network (column 12, lines 41-57 and column 13, lines 1-5).

As per claim 11, Shostack et al teach the determining the security characteristic operation further comprises:

monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a security alert message identifying the probed host as a security risk (column 7, lines 5-19), the security characteristic being a measure of connectivity between the first communications network and the second communications network (column 13, lines 1-

5).

As per claim 12, Shostack et al teach the second packet is derived using at least a portion of information from the transmitted packet (column 5, lines 24-45).

As per claim 15, Shostack et al teach the security characteristic includes an indication that the probed host is outside any security measures provide by a firewall associated with the communications network (column 9, lines 10-18).

As per clam 16, Shostack et al teach a communications system comprising:

a first plurality of computers associated with a first communications network;

a second plurality of computers associated with a second communications network, and

a security host computer which determines a security characteristic of a first computer from the plurality of computers, the security characteristic being a measure of connectivity between the first communications network and the second communications network (column 13, lines 1-5) performs a census of the communications network as a function of the first plurality of computers, and probes the first computer by transmitting a packet to the first computer, the first computer being selected from the census results and the packet being generated as a function of an IP address associated with a second computer of the second plurality of computers and an IP address associated

with the first computer, and determining a security level associated with the first computer as a function of a response of the first computer to receiving the packet (column 12, lines 41-57, column 1, lines 64-65, and column 3, lines 1-4).

As per claim 17, Shostack et al teach the security host computer is associated with the first communications network (column 4, lines 33-34).

As per claim 18, Shostack et al teach the response of the probed host to the receipt of the packet includes transmitting a second packet, the second packet being derived using at least a portion of information from the received packet (column 5, lines 20-35).

As per claim 19, Shostack et al teach the determining the security characteristic operation further comprises:

> monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a security alert message identifying the probed host as a security risk (column 7, lines 5-19).

As per claims 20 and 27, Shostack et al teach the first communications network is an intranet and the second communications network is an Internet (column 4, lines 14-21) and the two network communications have different security levels (column 13, lines 1-5).

As per claim 21, Shostack et al teach a security host computer comprising:

means for performing a census of a communications network and determining a topology of a first communications network, the topology being defined by at least One Computer (Column 12, lines 41 -57);

means for probing the at least One computer by transmitting a packet to the computer, the computer being selected from the census results and the packet being generated as a function of the topology, an IP address associated with a particular host computer associated with a second communications network and an IP address associated with the computer, the second communications network being separate from the first communications network (column 12, lines 41-57); and

a monitor for determining a security level of the computer as a function of a response by the computer to the receipt of the packet (column 12, lines 41-57) the security characteristic being a measure of connectivity between the first communications network and the second communications network (column 13, lines 1-5).

As per claim 22, Shostack et al teach the determining the security characteristic operation further comprises:

monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a

security alert message identifying the probed host as a security risk (column 7, lines 5-19).

As per claim 23, Shostack et al teach the security level is determined with respect to a firewall located between the first communications network and the second communications network (column 4, lines 14-21).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

sz
March 5, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100